# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/894,919 | 06/29/2001 | Robert Bruce Hirsh | 06975-200001/ Security 13 | 4606 |

26171 7590 06/03/2005

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

| EXAMINER | |
|---|---|
| CERVETTI, DAVID GARCIA | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

DATE MAILED: 06/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/894,919 | HIRSH, ROBERT BRUCE | |
| | Examiner | Art Unit | |
| | David G. Cervetti | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *08 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *20,21,24-28,30-39 and 55-95* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20,21,24-28,30-39 and 55-95* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/8/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Applicant's arguments filed March 8, 2005, have been fully considered but they are not persuasive.

### *Response to Amendment*

2. Examiner approves the amendment to the specification received on March 8, 2005. The objection to the drawings is withdrawn. The objection to the specification is withdrawn.

3. Cohen et al. relate to a single sign-on framework that **enables a user to sign on to multiple target systems and applications** (column 2, lines 60-67, column 3, lines 1-30) (emphasis added).

### *Claim Rejections - 35 USC § 102*

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**5. Claims 20-21, 25-26, 30-34, and 39 are rejected under 35 U.S.C. 102(e) as being anticipated by Cohen et al. (US Patent Number: 6,178,511).**

Regarding claim 20, Cohen et al. teach receiving a first request from a client at an intermediary, the first request relating to a request for access to the intermediary (column 6, lines 19-37); establishing a persistent connection between the client and the

intermediary in response to the first request from the client (column 6, lines 19-37); receiving a second request from the client at the intermediary, the second request relating to a request for access to a secured service (column 6, lines 60-67, column 7, lines 1-20); authenticating the intermediary to the secured service responsive to the second request (column 6, lines 60-67, column 7, lines 1-20); and enabling access by the client to the secured service conditioned on whether the intermediary is successfully authenticated to the secured service (column 6, lines 60-67, column 7, lines 1-20).

Regarding claim 21, Cohen et al. teach establishing the persistent connection with the client includes authenticating the client to the intermediary based on keystone authentication information provided by the client (column 6, lines 8-37); and authenticating the intermediary to the secured service is performed without provision by the client of authentication information duplicative or additional to the keystone information used to establish the persistent connection (column 6, lines 8-37).

Regarding claim 25, Cohen et al. teach receiving keystone authentication information from the client (column 6, lines 19-37); authenticating the client based on the keystone authentication information to provide a keystone authentication associated with the persistent connection (column 5, lines 1-15, column 6, lines 19-37); and establishing the persistent connection with the client based on the keystone authentication (column 5, lines 1-15, column 6, lines 19-37).

Regarding claim 26, Cohen et al. teach wherein the second request from the client for connection to the secured service is received after the persistent connection to the client is established (column 6, lines 60-67, column 7, lines 1-20).

Regarding claim 30, Cohen et al. teach wherein the intermediary comprises a persistent connection service that establishes the persistent connection with the client and a broker service that authenticates the intermediary to the secured service, and authenticating the intermediary includes the broker service receiving from the persistent connection service at a connection request address a communication based on the second request from the client and wherein the connection request address varies systematically with time (column 6, lines 60-67, column 7, lines 1-20).

Regarding claim 31, Cohen et al. teach wherein authenticating the intermediary to the secured service comprises: determining authorization information based on the second request from the client (column 6, lines 60-67, column 7, lines 1-20); communicating to the secured service an indication that the client desires to connect to the secured service, wherein the indication comprises the authorization information (column 6, lines 60-67, column 7, lines 1-20); receiving a response from the secured service indicating that the client may be allowed to establish the connection to the secured service by presenting the authorization information to the secured service (column 6, lines 60-67, column 7, lines 1-20); and enabling the client to present the authorization information to the secured service to establish the connection with the secured service (column 6, lines 60-67, column 7, lines 1-20).

Regarding claim 32, Cohen et al. teach wherein authenticating the intermediary to the secured service comprises: communicating, to the secured service, an indication that the client desires to connect to the secured service (column 6, lines 60-67, column 7, lines 1-20); receiving a response from the secured service indicating that the secured

service may accept a connection from the client, wherein the response includes authorization information (column 6, lines 60-67, column 7, lines 1-20); and communicating the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service (column 6, lines 60-67, column 7, lines 1-20).

Regarding claim 33, Cohen et al. teach wherein the authorization information is determined by the secured service (column 8, lines 63-67, column 9, lines 1-40).

Regarding claim 34, Cohen et al. teach authenticating the intermediary to the secured service comprises communicating with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service (column 6, lines 60-67, column 7, lines 1-20); the authorization information comprises constraint information (column 6, lines 60-67, column 7, lines 1-45, column 10, lines 20-45); and the authorization information may be ineffective to establish a connection with the secured service if the one or more connection constraints indicated by the constraint information are not satisfied (column 6, lines 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 39, Cohen et al. teach wherein the connection constraints include a constraint that the authorization information be presented to the secured service by a client for whom the connection was brokered (column 6, lines 60-67, column 7, lines 1-45, column 10, lines 20-45).

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**7. Claims 24, 27-28, 35-38, and 55-95 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al.**

Regarding claim 24, Cohen et al. do not disclose expressly wherein the intermediary is authenticated to the secured service before the client is enabled access to the secured service. However, Cohen et al. teach authenticating a user to an intermediary (column 6, lines 19-37), using this authentication information to establish a connection with secure resources (column 6, lines 37-67), and providing secure access to resources (column 6, lines 45-60, column 15, lines 1-25). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate the intermediary prior to permitting access to the secure resources to a user. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to authenticate systems and users prior to permitting access to resources.

Regarding claim 27, Cohen et al. do not disclose expressly wherein authenticating the intermediary to the secured service includes: providing a leveraged authentication based on the keystone authentication associated with the persistent connection; and using the leveraged authentication to establish the connection with the

secured service. However, Cohen et al. teach authenticating a user to an intermediary (column 6, lines 19-37), using this authentication information to establish a connection with secure resources (column 6, lines 37-67), and providing secure access to resources (column 6, lines 45-60, column 15, lines 1-25). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate the intermediary prior to permitting access to the secure resources to a user. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to authenticate systems and users prior to permitting access to resources.

Regarding claim 28, Cohen et al. teach wherein the keystone authentication is used to provide the leveraged authentication without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection (column 6, lines 60-67, column 7, lines 1-20).

Regarding claim 35, Cohen et al. do not disclose expressly wherein the connection constraints include a constraint that limits a number of uses for the authorization information to a predetermined threshold number. However, Examiner takes Official Notice that the use of a threshold number to limit use of authorization information was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a constraint that limits a number of uses for the authorization information to a predetermined threshold number since Examiner takes Official Notice that the use of a

threshold number to limit use of authorization information was conventional and well known.

Regarding claim 36, Cohen et al. do not disclose expressly wherein the connection constraints include a constraint that the number of times that the authorization information has been used not exceed a predetermined number of times. However, Examiner takes Official Notice that the use of a threshold number to limit use of authorization information was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a constraint that the number of times that the authorization information has been used not exceed a predetermined number of times since Examiner takes Official Notice that the use of a threshold number to limit use of authorization information was conventional and well known.

Regarding claim 37, Cohen et al. do not disclose expressly wherein the connection constraints include a one-time-use password. However, Examiner takes Official Notice that the use of one-time passwords was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a one-time-use password since Examiner takes Official Notice that the use of one-time passwords was conventional and well known.

Regarding claim 38, Cohen et al. do not disclose expressly wherein the connection constraints include a constraint that the authorization information be used within a predetermined time window. Cohen et al. teach the use of targets that have time limited credentials (column 13, lines 30-45). Therefore, it would have been obvious

to one having ordinary skill in the art at the time the invention was made to include a constraint that the authorization information be used within a predetermined time window. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to limit access to resources based on specific times.

Regarding claim 55, Cohen et al. do not disclose expressly wherein enabling access by the client to the secured service comprises enabling the client to access the secured service independent of the intermediary. However, Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use client-server communications independent of an intermediary since Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known.

Regarding claim 56, Cohen et al. do not disclose expressly wherein enabling the client to access the secured service comprises enabling the client to leverage a connection other than the persistent connection established between the client and the intermediary. However, Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use client-server communications independent of an intermediary since Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known.

Regarding claim 57, Cohen et al. teach wherein enabling the client to access the secured service comprises providing constrained authentication information to the client (column 5, lines 5-67, column 6, lines 19-37, 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 58, Cohen et al. teach wherein the constrained authentication information is provided to the intermediary by the secured service (column 5, lines 5-67, column 6, lines 19-37, 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 59, Cohen et al. teach wherein the constrained authentication information is determined by the intermediary and authenticated by the secured service (column 5, lines 5-67, column 6, lines 19-37, 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 60, Cohen et al. do not disclose expressly wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel. Cohen et al. do teach an application "Global Sign On" (column 4, lines 1-10, figures 4-5, columns 5-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel as clients. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use one or more of a web browser, an e-mail

client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel as clients.

Regarding claim 61, Cohen et al. do not disclose expressly wherein the intermediary comprises one or more of an instant messaging service, an e-mail service. Cohen et al. do teach an application "Global Sign On", a login service, an authentication service, an authorization service, a persistent connection service, and a broker service (column 4, lines 1-10, figures 4-5, columns 5-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use one or more of an instant messaging service, an e-mail service as intermediaries. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use one or more of an instant messaging service, an e-mail service as intermediaries to access secured resources.

Regarding claim 62, Cohen et al. teach wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service (column 4, lines 20-35).

Regarding claim 63, Cohen et al. do not disclose expressly wherein the intermediary is authenticated to the secured service as a consequence of the second request. However, Cohen et al. teach authenticating a user to an intermediary (column 6, lines 19-37), using this authentication information to establish a connection with secure resources (column 6, lines 37-67), and providing secure access to resources

(column 6, lines 45-60, column 15, lines 1-25). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate the single sign-on system of Cohen et al. prior to permitting access to the secure resources to a user. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to authenticate systems and users prior to permitting access to resources.

Regarding claim 64, Cohen et al. teach wherein the request for access to the secured service comprises an explicit request for access by the client (column 5, lines 5-67, column 6, lines 19-37, 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 65, Cohen et al. teach wherein the request for access to the secured service comprises a client communication received via the secured service (column 6, lines 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 66, Cohen et al. do not disclose expressly wherein the secured service is available for direct authentication by a user without establishing a persistent connection between the user and the intermediary. However, Examiner takes Official Notice that the use of direct authentication by a user was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use direct authentication by a user to the secured service since Examiner takes Official Notice that the use of direct authentication by a user was conventional and well known.

Regarding claim 67, Cohen et al. teach a method, performed by a client, of leveraging a connection with an intermediary to access a secured service, the method

comprising: receiving a user request for access to a secured service (column 6, lines 60-67, column 7, lines 1-45, column 10, lines 20-45); submitting, by the client, a request, which is based on the user request for access to a secured service, to an intermediary that is physically distinct of the secured service (column 6, lines 60-67, column 7, lines 1-45, column 10, lines 20-45); receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request (column 6, lines 19-37). Cohen et al. do not disclose explicitly submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary. However, Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use client-server communications independent of an intermediary since Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known.

Regarding claim 68, Cohen et al. teach wherein establishing the authenticated connection between the client and the intermediary comprises: sending, by the client, keystone authentication information to the intermediary; and receiving, from the intermediary, verification of the keystone authentication information (column 5, lines 5-67, column 6, lines 19-37, 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 69, Cohen et al. do not disclose expressly wherein submitting the request to the intermediary for access to the secured service prompts the intermediary to authenticate itself to the secured service without provision by the client of authentication information duplicative or additional to the keystone information. However, Cohen et al. teach authenticating a user to an intermediary (column 6, lines 19-37), using this authentication information to establish a connection with secure resources (column 6, lines 37-67), and providing secure access to resources (column 6, lines 45-60, column 15, lines 1-25). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate the intermediary prior to permitting access to the secure resources to a user. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to authenticate systems and users prior to permitting access to resources.

Regarding claim 70, Cohen et al. do not disclose expressly wherein the intermediary is authenticated to the secured service by provision, by the intermediary, of a leveraged authentication based on the keystone authentication. However, Cohen et al. teach authenticating a user to an intermediary (column 6, lines 19-37), using this authentication information to establish a connection with secure resources (column 6, lines 37-67), and providing secure access to resources (column 6, lines 45-60, column 15, lines 1-25). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate the system of Cohen et al. prior to permitting access to the secure resources to a user by submitting authentication information to the secured service. One of ordinary skill in the art would have been

motivated to do so because it was well known in the art to authenticate systems and users prior to permitting access to resources.

Regarding claim 71, Cohen et al. teach wherein the constrained authorization information has been issued by the secured service and sent by the secured service to the intermediary (column 5, lines 1-15).

Regarding claim 72, Cohen et al. teach wherein the constrained information has been provided by the intermediary and authenticated by the secured service (column 5, lines 1-15).

Regarding claim 73, Cohen et al. do not disclose expressly wherein the constrained authorization information comprises one or more of a constraint that the authorization information has been used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client. However, Examiner takes Official Notice that the use of a threshold number, a time window, and to receive the information from the client attempting access to information, to limit use of authorization information was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to user either of these constraints since Examiner takes Official Notice that the use of one-time passwords was conventional and well known.

Regarding claim 74, Cohen et al. do not disclose expressly wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and

an operating system kernel. Cohen et al. do teach an application "Global Sign On" (column 4, lines 1-10, figures 4-5, columns 5-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel as clients. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel as clients.

Regarding claim 75, Cohen et al. do not disclose expressly wherein the intermediary comprises one or more of an instant messaging service, an e-mail service. Cohen et al. do teach an application "Global Sign On", a login service, an authentication service, an authorization service, a persistent connection service, and a broker service (column 4, lines 1-10, figures 4-5, columns 5-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use one or more of an instant messaging service, an e-mail service as intermediaries. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use one or more of an instant messaging service, an e-mail service as intermediaries to access secured resources.

Regarding claim 76, Cohen et al. teach wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system

kernel, an authentication service, an authorization service, and a persistent connection service (column 4, lines 20-35).

Regarding claim 77, Cohen et al. teach wherein the client request for access to the secured service comprises an explicit request for access by the client (column 5, lines 5-67, column 6, lines 19-37, 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 78, Cohen et al. teach wherein the client request for access to the secured service comprises a communication sent by the client to the intermediary via the secured service (column 5, lines 5-67, column 6, lines 19-37, 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 79, Cohen et al. do not disclose expressly wherein the secured service is available for direct authentication by a user without the user establishing an authenticated connection between the user and the intermediary. However, Examiner takes Official Notice that the use of direct authentication by a user was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use direct authentication by a user to the secured service since Examiner takes Official Notice that the use of direct authentication by a user was conventional and well known.

Regarding claim 80, Cohen et al. do not disclose expressly wherein the direct authenticated connection between the client and the secured service is established by leveraging a connection other than the authenticated connection between the client and the intermediary. However, Examiner takes Official Notice that the use of direct authentication by a user was conventional and well known. Therefore, it would have

been obvious to one having ordinary skill in the art at the time the invention was made to use direct authentication by a user to the secured service since Examiner takes Official Notice that the use of direct authentication by a user was conventional and well known.

Regarding claim 81, Cohen et al. teach a method, performed by a secured service, of allowing a client access based on an authenticated connection between the client and an intermediary, the method comprising: receiving, at a secured service and from an intermediary, notification of a request by a client to access the secured service (column 6, lines 60-67, column 7, lines 1-45, column 10, lines 20-45). Cohen et al. do not disclose explicitly determining whether a trusted relationship exists between the secured service and the intermediary, responsive to the client request; and conditioned on the existence of a trusted relationship between the secured service and the intermediary, enabling access by the client to the secured service. However, Examiner takes Official Notice that the use of "trusted connections" was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a "trusted connection" between the Single Sign-On system of Cohen et al. and the target resources since Examiner takes Official Notice that the use of "trusted connections" was conventional and well known.

Regarding claim 82, Cohen et al. teach wherein enabling access by the client comprises issuing constrained authorization information to the intermediary for use by the client to access the secured service (column 5, lines 5-67).

Regarding claim 83, Cohen et al. teach wherein enabling access by the client further comprises receiving the constrained authorization information from the client (column 5, lines 5-67).

Regarding claim 84, Cohen et al. do not disclose expressly wherein the constrained authorization information comprises one or more of a constraint that the authorization information be used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client. However, Examiner takes Official Notice that the use of a threshold number, a time window, and to receive the information from the client attempting access to information, to limit use of authorization information was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to user either of these constraints since Examiner takes Official Notice that the use of one-time passwords was conventional and well known.

Regarding claim 85, Cohen et al. teach wherein enabling access by the client comprises authenticating constrained authorization information to be provided by the intermediary to the client to access the secured service (column 6, lines 1-37).

Regarding claim 86, Cohen et al. teach wherein enabling access by the client further comprises receiving the constrained authorization information from the client (column 6, lines 60-67, column 7, lines 1-45, column 10, lines 20-45).

Regarding claim 87, Cohen et al. do not disclose expressly wherein the constrained authorization information comprises one or more of a constraint that the

authorization information be used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client. However, Examiner takes Official Notice that the use of a threshold number, a time window, and to receive the information from the client attempting access to information, to limit use of authorization information was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to user either of these constraints since Examiner takes Official Notice that the use of one-time passwords was conventional and well known.

Regarding claim 88, Cohen et al. do not disclose expressly wherein enabling access by the client comprises establishing a connection with the client independent of the intermediary. However, Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use client-server communications independent of an intermediary since Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known.

Regarding claim 89, Cohen et al. do not disclose expressly wherein the connection between the client and the secured service is established by the client leveraging a connection other than a connection between the client and the intermediary. However, Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use client-server communications independent of an intermediary since Examiner takes Official Notice that the use of client-server communications independent of an intermediary was conventional and well known.

Regarding claim 90, Cohen et al. do not disclose expressly wherein determining whether a trusted relationship exists between the secured service and the intermediary comprises receiving authentication information from the intermediary. However, Examiner takes Official Notice that the use of "trusted connections" was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a "trusted connection" between the Single Sign-On system of Cohen et al. and the target resources and to authenticate the Single Sign-On system since Examiner takes Official Notice that the use of "trusted connections" was conventional and well known.

Regarding claim 91, Cohen et al. teach wherein the intermediary provides the authentication information to the secured service without provision by the client of other authentication information that is duplicative or additional to keystone authentication information provided by the client to the intermediary to establish the authenticated connection between the client and the intermediary (column 6, lines 60-67, column 7, lines 1-20).

Regarding claim 92, Cohen et al. do not disclose expressly wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and

an operating system kernel. Cohen et al. do teach an application "Global Sign On" (column 4, lines 1-10, figures 4-5, columns 5-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel as clients. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel as clients.

Regarding claim 93, Cohen et al. do not disclose expressly wherein the intermediary comprises one or more of an instant messaging service, an e-mail service. Cohen et al. do teach an application "Global Sign On", a login service, an authentication service, an authorization service, a persistent connection service, and a broker service (column 4, lines 1-10, figures 4-5, columns 5-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use one or more of an instant messaging service, an e-mail service as intermediaries. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use one or more of an instant messaging service, an e-mail service as intermediaries to access secured resources.

Regarding claim 94, Cohen et al. teach wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system

kernel, an authentication service, an authorization service, and a persistent connection service (column 4, lines 20-35).

Regarding claim 95, Cohen et al. do not disclose expressly wherein the secured service is available for direct authentication by a user without determining whether a trusted relationship exists between the secured service and the intermediary. However, Examiner takes Official Notice that the use of direct authentication by a user was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use direct authentication by a user to the secured service since Examiner takes Official Notice that the use of direct authentication by a user was conventional and well known.

***Conclusion***

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100